UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

In re Flagstar December 2021 Data Security Incident Litigation	Case No. 4:22-cv-11385 Hon. Shalina D. Kumar Magistrate Judge Kimberly G. Altman **DEFENDANTS' MOTION TO DISMISS THE CONSOLIDATED CLASS ACTION COMPLAINT**

Pursuant to Federal Rule of Civil Procedure 12(b)(1) and (6), Defendants New York Community Bancorp, Inc., f/k/a Flagstar Bancorp, Inc. and Flagstar Bank, N.A., f/k/a Flagstar Bank, FSB (together, "Defendants" or "Flagstar"), through their undersigned counsel, respectfully move to dismiss the Consolidated Class Action Complaint (the "Complaint") under Federal Rule of Civil Procedure 12(b)(1) and (6). For the reasons set forth more fully in the attached brief, dismissal of the Complaint is warranted because Plaintiffs lack Article III standing and fail to state a claim upon which relief may be granted.

On July 21, 2023, pursuant to Local Civil Rule 7.1(a), Defendants' counsel held a conference with interim lead counsel in which Defendants' counsel explained the nature of the motion and its legal basis and requested but did not obtain concurrence in the relief sought.

WHEREFORE, for these reasons and those stated more fully in the accompanying brief, Flagstar respectfully requests that the Court grant its Motion to Dismiss the Consolidated Class Action Complaint and dismiss the Complaint in its entirety, and award any other relief to which Flagstar may be entitled, and the Court deems appropriate, under the circumstances.

Dated: July 24, 2023

Respectfully submitted,

/s/ William E. Ridgway
William E. Ridgway
Lindsey Sieling
SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP
155 N. Wacker Dr., Suite 2700
Chicago, IL 60606
Telephone: (312) 407-0700
Facsimile: (312) 407-0411
William.Ridgway@skadden.com
Lindsey.Sieling@skadden.com

Sean P. McNally (P66292)
Jason E. Manning
TROUTMAN PEPPER HAMILTON SANDERS LLP
4000 Town Center, Suite 1800
Southfield, MI 48075
Telephone: (248) 359-7300
Sean.McNally@troutman.com
Jason.Manning@troutman.com

Counsel for Defendants

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

In re Flagstar December 2021 Data Security Incident Litigation	Case No. 4:22-cv-11385 Hon. Shalina D. Kumar Magistrate Judge Kimberly G. Altman **BRIEF IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS THE CONSOLIDATED CLASS ACTION COMPLAINT**

TABLE OF CONTENTS

Page

ISSUES PRESENTED

1. Whether Plaintiffs failed to establish Article III standing by claiming only a risk of future harm and purported injuries that are not fairly traceable to the Cyber Incident that Flagstar suffered.

2. Whether Plaintiffs failed to state a claim for which relief can be granted under any of the eighteen causes of action alleged in the Complaint.

CONTROLLING OR MOST APPROPRIATE AUTHORITIES

Section I

1. Federal Rule of Civil Procedure 12(b)(1)
2. *Ashcroft v. Iqbal*, 556 U.S. 662 (2009)
3. *Cartwright v. Garner*, 751 F.3d 752 (6th Cir. 2014)
4. *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013)
5. *Garland v. Orlans, PC*, 999 F.3d 432 (6th Cir. 2021)
6. *Lujan v. Defenders of Wildlife*, 504 U.S. 555 (1992)
7. *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021)
8. *Ward v. Nat'l Patient Acct. Servs. Sols., Inc.*, 9 F.4th 357 (6th Cir. 2021)
9. *Whitmore v. Arkansas*, 495 U.S. 149 (1990)

Section II

10. Federal Rule of Civil Procedure 12(b)(6)
11. *Bank of Am., N.A. v. First Am. Title Ins. Co.*, 499 Mich. 74, 878 N.W.2d 816 (2016)
12. *Doe v. Henry Ford Health System*, 308 Mich. App. 592, 865 N.W.2d 915 (2014)
13. *Rakyta v. Munson Healthcare*, No. 354831, 2021 WL 4808339 (Mich. Ct. App. Oct. 14, 2021)
14. *16630 Southfield Ltd. P'ship v. Flagstar Bank, F.S.B.*, 727 F.3d 502 (6th Cir. 2013)

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Rules

Regulations

PRELIMINARY STATEMENT

Flagstar suffered a ransomware attack in December 2021 in which cyber criminals stole certain data (the "Cyber Incident"). In order to protect customers, Flagstar opted to pay the ransom, allowing Flagstar to delete entirely the data the cyber criminals stole. To this day, a year and a half after the incident, none of that data has ever been made available on the dark web.

Just one week after public announcement of the Cyber Incident, plaintiffs began filing cookie-cutter lawsuits against Flagstar. Those suits were consolidated, and Plaintiffs have now filed a Consolidated Class Action Complaint (the "Complaint"), alleging that their personally identifiable information ("PII") was compromised in the Cyber Incident.

Despite the litany of claimed injuries Plaintiffs conjure up, none amounts to a concrete injury fairly traceable to the Cyber Incident. This crucial gap is not an oversight. The truth is that the stolen data was never misused or made available on the dark web so any claimed injuries will never be more than theoretical and this suit runs squarely into bedrock principles of Article III standing. The claims cannot survive a facial or factual attack on standing and dismissal is warranted.

Plaintiffs also fail to state a claim upon which relief may be granted. Each of Plaintiffs' eighteen claims fails as a matter of law for the following reasons:

Negligence and negligence per se: (1) Plaintiffs have not adequately

alleged that Flagstar committed a negligent act or omission, (2) negligence per se is not an independent cause of action, (3) the majority of Plaintiffs fail to allege cognizable injuries, and (4) all Plaintiffs fail to allege a sufficient causal link between any negligent act by Flagstar and their purported injuries.

Breach of confidence: (1) Breach of confidence is not recognized as a separate tort under Michigan law, (2) Plaintiffs have not alleged the requisite intentional disclosure, and (3) Plaintiffs fail to allege any resulting damages.

Invasion of Privacy: (1) Plaintiffs have not alleged the requisite intent, and (2) Plaintiffs fail to allege any resulting damages.

Breach of implied and express contract: (1) Plaintiffs have not alleged a valid express or implied contract, (2) any contract is unenforceable because it is not in writing and signed by Flagstar, (3) Plaintiffs allege no credible breach, and (4) Plaintiffs fail to allege any resulting damages.

Unjust Enrichment: Plaintiffs fail to allege that Flagstar (1) received any benefit from Plaintiffs, and (2) retention of that purported benefit would be unjust.

Declaratory Judgment: (1) Declaratory judgment is not an independent cause of action, and (2) Plaintiffs fail to allege a certainly impending injury.

California Consumer Privacy Act: California Plaintiffs (1) do not adequately allege that Flagstar did not maintain reasonable security procedures, and (2) failed to fulfill the pre-suit notice requirement.

Data Breach Notification Statutes (CA, CO, WA): Plaintiffs do not allege that (1) any of their injuries arose from delayed notice, or (2) that any purported delay in disclosure was unreasonable, and (3) the Colorado Security Breach Notification Act lacks a private right of action.

State Consumer Fraud and Unfair and Deceptive Acts and Practices Laws (CA, CO, IN, MI, WA): (1) Plaintiffs fail to allege a cognizable injury caused by the alleged violation, (2) the fraud-based claims fail to satisfy Rule 9(b), (3) Plaintiffs fail to plead an unfair or unlawful practice, (4) the California Unfair Competition Law claim fails because California Plaintiffs do not lack an adequate legal remedy, and (5) the Indiana Deceptive Consumer Sales Act claim fails because there is no allegation that Flagstar acted with intent to defraud and a claim cannot be based on a purported delay in notification.

BACKGROUND[1]

Flagstar is a Michigan-based bank with its regional headquarters in Troy, Michigan. *See* ECF No. 52, Compl. ¶ 5, PageID.546-47. On December 3 and 4, 2021, cyber criminals gained unauthorized access to Flagstar's network and stole certain data. *Id.*; Ex. A ¶ 3. Flagstar promptly activated its incident response plan,

[1] The facts are taken from the Complaint and the declarations of Jennifer Charters and William Hardin, attached hereto as Exhibits A and B, respectively. The declarations are used only for the factual challenge to Article III standing and not for the motion to dismiss under Rule 12(b)(6).

engaged external cybersecurity professionals experienced in handling these types of incidents, and reported the matter to federal law enforcement. Compl. ¶ 35, PageID.562-63.

Flagstar soon after received a ransom demand from the cyber criminals and, following negotiations, Flagstar agreed to pay $1 million in exchange for, among other things, the complete deletion of all data acquired from Flagstar's network. Ex. A ¶ 4. On December 31, 2021, Flagstar paid $1 million, and Flagstar was given access to the server where the stolen data was stored, which Flagstar deleted. *Id.* ¶¶ 5-6. In the time since this incident, Flagstar's cybersecurity experts have continued to monitor the dark web, including the site associated with the cyber criminals, and none of the stolen data has been released. *Id.* ¶ 8.

Following an extensive forensic investigation and manual review of the exposed data, Flagstar concluded that the data the cyber criminals temporarily possessed included PII of around 1.5 million people. Compl. ¶ 36, PageID.563. Even though there was no evidence that any PII had been misused (indeed, the criminals no longer possessed the stolen data), Flagstar still offered impacted individuals two years of free credit monitoring services. *Id.* ¶¶ 40, 43, PageID.565-66. Within a week of offering these services, the first lawsuit was filed by Philip Angus, who—along with Plaintiff Mark Wiedder—had filed a nearly identical complaint against Flagstar in March 2021 relating to a data incident involving

Accellion's file transfer platform, which was used by Flagstar to securely transfer sensitive data (the "Accellion Incident").[2] *See* ECF No. 1, PageID.1; *Angus v. Flagstar Bank, FSB*, No. 2:21-CV-10657-MFL-DRG, ECF No. 1, PageID.1. Following consolidation of the cases filed in the Eastern District of Michigan relating to the Cyber Incident, Plaintiffs filed their consolidated Complaint.

Plaintiffs are twelve current and former customers of Flagstar who allege that Flagstar's purported negligence led to their PII being compromised. Compl. ¶¶ 8-19, PageID.548-56. Plaintiffs reside in seven different states—California (Smith, Kennedy, Tallman, and Wiedder), Colorado (McCarthy), Florida (Hernandez), Indiana (Worton), Michigan (Nasrallah, Silva, and Scanlon), Missouri (Turner), and Washington (McLaughlin)—and assert eighteen causes of action.

Eight Plaintiffs—Smith, Tallman, Wiedder, McCarthy, Nasrallah, Silva, Scanlon, and Turner—allege injuries related to purported misuse of their PII. In particular, Plaintiff Smith claims to have suffered fraud in the form of unauthorized attempted bank transfers; Plaintiff Silva alleges that he experienced multiple unauthorized withdrawals from his banking cards; Plaintiff Scanlon alleges that she suffered fraudulent charges on her bank account; Plaintiff Nasrallah asserts he experienced unauthorized tax returns and fraudulent credit inquiries; and Plaintiffs

[2] Philip Angus is no longer a named plaintiff in the Complaint.

Tallman, Wiedder, McCarthy, and Turner allege that they have received an increase in spam calls, text messages, emails and/or solicitations. *Id.* ¶¶ 8, 10-12, 15-18, PageID.548-55. But none of these allegations is remotely plausible. Plaintiff Smith's bank account information, Plaintiff Wiedder's phone number, and Plaintiff Silva's banking card information *were not compromised* during the Cyber Incident. Ex. A ¶ 10. And no personal information associated with Plaintiff Tallman or Plaintiff McCarthy was compromised during the Cyber Incident. *Id*.

All Plaintiffs also allege a variety of other injuries unrelated to claimed misuse of their PII. They claim to have lost time and money responding to the Cyber Incident, including: researching the breach, reviewing bank accounts and credit reports, signing up for and/or monitoring credit monitoring services,[3] notifying banks and other entities about the Cyber Incident, and placing credit freezes and fraud alerts. Compl. ¶¶ 8-19, PageID.547-56. Plaintiffs also allege harm in the form of (i) lost or reduced value of their PII, (ii) loss of privacy rights, (iii) overpayment to Flagstar for services purchased (though Plaintiffs do not allege what services were purchased or the cost), and (iv) "certain, imminent, and ongoing threat of fraud and identity theft." *Id.* ¶ 86, PageID.586.

[3] Only two Plaintiffs—Worton and Turner—allege that they purchased credit monitoring services as a result of the Cyber Incident. Compl. ¶¶ 14, 18, PageID.552, 554-55. Other Plaintiffs purchased credit monitoring prior to the Cyber Incident and now allege that they will need to continue paying for these services indefinitely. *Id.* ¶¶ 9-10, 16-17, PageID.549-50, 553-54.

While Plaintiffs allege on "information and belief" that the PII compromised in the Cyber Incident was "made available to other criminals on the dark web," *id.* ¶ 6, PageID.547, that allegation is flatly wrong. In fact, the stolen data was deleted by Flagstar and was never released or posted on the dark web. Ex. A ¶¶ 6-8. Flagstar also retained William Hardin from CRA International, Inc. ("CRA"), a cybersecurity and ransomware expert, to analyze the dark web. Ex. B ¶ 9. Mr. Hardin further confirms that the cyber criminals responsible for the Cyber Incident have not posted to the dark web any data acquired during the Cyber Incident. *Id.* ¶ 27. The only Flagstar data located on the dark web relates to postings by the CL0P ransomware group, which was responsible for the Accellion Incident.[4] *Id.* ¶¶ 24, 26.

CRA also analyzed information on the dark web related to Plaintiff John Scott Smith. *Id.* ¶ 29. CRA found Plaintiff Smith's information within *thirteen* previously reported data breaches that involved companies other than Flagstar. *Id.* ¶ 34. Some of those data breaches included Plaintiff Smith's passwords, which were found to be very weak and susceptible to brute-force attacks. *Id.* ¶ 36. CRA did not find any of Plaintiff Smith's data from the Cyber Incident available on the dark web, but did find his data from the Accellion Incident. *Id.* ¶¶ 32-33.

[4] Seven Plaintiffs—Smith, Kennedy, Wiedder, Hernandez, Nasrallah, Silva, and Turner—had PII compromised in the Accellion Incident. Ex. A ¶ 12.

LEGAL STANDARD

Flagstar moves to dismiss the Complaint under Federal Rule of Civil Procedure 12(b)(1) for lack of standing. At the pleading stage, a plaintiff must allege facts demonstrating, "(i) that he suffered an injury in fact that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant; and (iii) that the injury would likely be redressed by judicial relief." *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2203 (2021). "Allegations of *possible* future injury do not satisfy the requirements of Art. III." *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990) (emphasis added). Rather, a "threatened injury must be 'certainly impending' to constitute injury in fact." *Id.* (citation omitted). The injury must also be "'fairly . . . trace[able] to the challenged action of the defendant, and not . . . th[e] result [of] the independent action of some third party not before the court.'" *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992) (ellipsis and alterations in original) (quoting *Simon v. E. Ky. Welfare Rights Org.*, 426 U.S. 26, 41-42 (1976)). A "speculative chain of possibilities does not establish that [the] injury . . . is fairly traceable." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013). A "plaintiff[] must demonstrate standing for each claim that they press and for each form of relief that they seek (for example, injunctive relief and damages)." *TransUnion*, 141 S. Ct. at 2208.

A Rule 12(b)(1) motion for lack of subject matter jurisdiction may be a

facial attack—which challenges the sufficiency of the pleading itself—or a factual attack—which challenges the factual existence of subject matter jurisdiction. *Cartwright v. Garner*, 751 F.3d 752, 759–60 (6th Cir. 2014). When analyzing a facial attack, "the court takes the allegations of the complaint as true." *Id.* (citation omitted). "In the case of a factual attack, a court has broad discretion with respect to what evidence to consider in deciding whether subject matter jurisdiction exists, including evidence outside of the pleadings, and has the power to weigh the evidence and determine the effect of that evidence on the court's authority to hear the case." *Id.*

Flagstar also moves to dismiss under Rule 12(b)(6) for failure to state a claim. To survive a Rule 12(b)(6) motion to dismiss, a complaint must contain "sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citation omitted). "[A] plaintiff cannot overcome a Rule 12(b)(6) motion to dismiss simply by referring to conclusory allegations in the complaint that the defendant violated the law." *16630 Southfield Ltd. P'ship v. Flagstar Bank, F.S.B.*, 727 F.3d 502, 504 (6th Cir. 2013). This "pleading standard is particularly demanding in 'complex, large-scale' data breach class action litigation." *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 972 (S.D. Cal. 2014) (citation omitted).

ARGUMENT

I. Plaintiffs Fail to Establish a Concrete Injury in Fact Traceable to the Cyber Incident, and Therefore Lack Standing Under Article III.

Plaintiffs fail to plead—and, based on extrinsic evidence, cannot establish—a concrete injury traceable to the Cyber Incident. Plaintiffs' alleged injuries fall into two broad categories: (i) injuries allegedly caused by the actual misuse of certain Plaintiffs' PII, and (ii) injuries unrelated to actual misuse of Plaintiffs' PII, including the risk of future identity theft and fraud, time and money spent monitoring financial accounts and purchasing credit monitoring services, lost value of PII, loss of privacy, and overpayment for services received from Flagstar. None of these alleged injuries can survive either a facial or factual attack on standing.

A. Plaintiffs Fail to Adequately Allege That Purported Misuse of PII Constitutes an Injury That Is Traceable to the Cyber Incident.

Eight Plaintiffs—Smith, Tallman, Wiedder, McCarthy, Nasrallah, Silva, Scanlon and Turner—claim "injuries" related to purported misuse of their PII. None of these Plaintiffs, however, alleges any facts connecting their claimed "injuries" to the Cyber Incident, which is not surprising because their PII was never in fact misused. Tellingly, Plaintiffs neglect to allege: (1) the PII they believe was compromised in the Cyber Incident, (2) when the purported misuse of their PII occurred (including that it even post-dated the incident), or (3) that their PII has not been previously compromised in other security incidents. This pleading failure is significant given the prevalence of data breaches. *See* Compl. ¶¶ 54-56,

PageID.570-572 (alleging that billions of sensitive records have been exposed in various data breach incidents over the past ten years).

Plaintiff Smith, for example, alleges that he experienced "unauthorized *attempted* bank transfers" across multiple banks and accounts. Compl. ¶ 8, PageID.548 (emphasis added). Even if "attempted" unauthorized activity could constitute an injury, which it cannot,[5] Plaintiff Smith has not alleged that he even gave Flagstar information about those bank accounts, let alone that such information was actually compromised in the Cyber Incident (in fact it was not). The alleged attempted fraudulent activity thus lacks any "logical connection to the data" that was purportedly accessed. *In re Cmty. Health Sys., Inc.*, No. 15-CV-222-KOB, 2016 WL 4732630, at *12 (N.D. Ala. Sept. 12, 2016) (attempted theft of funds from checking account and unauthorized charges not traceable to defendant because data breach did not include financial information).

Plaintiff Silva likewise alleges that he experienced unauthorized withdrawals from his banking cards, and Plaintiff Scanlon alleges that she experienced unauthorized access and charges to her bank account. Compl. ¶¶ 16-17, PageID.553-54. Yet these plaintiffs also fail to allege they provided their bank card/account information to Flagstar, that the card/account information was

[5] *See Whalen v. Michaels Stores, Inc.*, 689 F. App'x 89, 90 (2d Cir. 2017) (concluding that unsuccessful attempts to use a compromised credit card number did not constitute an injury).

compromised in the Cyber Incident, or that these unauthorized withdrawals or charges occurred after the Cyber Incident. Their allegations therefore also lack any "logical connection" to the Cyber Incident. *See McCombs v. Delta Grp. Elecs., Inc.*, No. 1:22-CV-00662-MLG-KK, 2023 WL 3934666, at *6 (D.N.M. June 9, 2023) (no causal connection inferred between alleged bank account access and data breach where plaintiff did not identify, among other things, the exact dates and details of the alleged unauthorized access).

Plaintiff Nasrallah alleges that (1) unauthorized financial accounts were opened in his name, (2) unauthorized tax returns were filed in his name, and (3) several fraudulent inquiries of his credit were made. Compl. ¶ 15, PageID.552-53. Again, Plaintiff Nasrallah does not allege what PII was compromised in the Cyber Incident, that the purported fraudulent acts occurred after the Cyber Incident, or that his PII has not been compromised in other data breaches.

Plaintiffs Tallman, Wiedder, McCarthy, Scanlon, and Turner allege an increase in "suspicious" spam calls, text messages, emails, mail and/or solicitations. Compl. ¶¶ 10-12, 17-18, PageID.549-51, 554-55. Courts, however, "have generally rejected the theory that unsolicited calls or emails constitute an injury in fact." *Cooper v. Bonobos, Inc.*, No. 21-CV-854 (JMF), 2022 WL 170622, at *5 (S.D.N.Y. Jan. 19, 2022); *see also McCombs*, 2023 WL 3934666, at *6 (collecting cases). But even if these allegations were enough to plead an injury in

fact, Plaintiffs have not plausibly linked this alleged harm to the Cyber Incident. Receiving spam calls or emails, "while perhaps 'consistent with' data misuse, does not 'plausibly suggest' that any actual misuse of Plaintiff's personal identifying information has occurred." *Legg v. Leaders Life Ins. Co.*, 574 F. Supp. 3d 985, 993 (W.D. Okla. 2021). This is especially true where Plaintiff Wiedder has made a nearly identical allegation of increased spam calls related to a *different* cyber incident. *Angus v. Flagstar Bank, FSB*, No. 2:21-cv-10657-MFL-DRG, Dkt. No. 38, Second Consolidated Class Compl. ¶ 99, PageID.458 (E.D. Mich. filed Aug. 12, 2021) ("[S]ince January 2021, Plaintiff Wiedder and his spouse have experienced an increase in the volume of 'spam' calls they receive.").

Finally, Plaintiffs Wiedder's and Turner's bare allegations that their PII was found on the dark web, Compl. ¶¶ 11, 18, PageID.550-51, 554-55, are insufficient to confer standing. *See Blood v. Labette Cnty. Med. Ctr.*, No. 5:22-CV-04036-HLT-KGG, 2022 WL 11745549, at *8 (D. Kan. Oct. 20, 2022) (allegation that plaintiffs' PII had been found on the "dark web" "lacks a plausible connection to Defendant's actions"). In sum, Plaintiffs fail to plausibly allege that any purported instance of misuse of PII is fairly traceable to the Cyber Incident.

B. Extrinsic Evidence Establishes That Purported Misuse of PII Is Not Traceable to the Cyber Incident.

Extrinsic evidence confirms why Plaintiffs uniformly fail to identify any facts that connect their claimed injuries to the Cyber Incident. *First*, the Cyber

Incident involved a ransomware attack in which Flagstar paid the ransom, deleted the exfiltrated data from the cyber criminal's server, and received confirmation that there were no additional copies of the data. *See* Ex. A ¶¶ 4-6.

Second, data from the Cyber Incident was *never* available on the dark web. Flagstar's cybersecurity vendor monitored the dark web, including a site associated with the cyber criminals, and Flagstar's data was never released. *Id.* ¶ 8. Independent experts have also confirmed that the data from the Cyber Incident is not available on the dark web. Ex. B ¶ 27. In fact, the only Flagstar data found on the dark web relates to the Accellion Incident. *Id.* ¶¶ 24, 26.

Third, for several Plaintiffs, the purported PII they claim was misused was definitively *not* compromised in the Cyber Incident. For example, Plaintiff Smith's bank account information, Plaintiff Silva's bank card information, and Plaintiff Wiedder's phone number were not compromised in the Cyber Incident. Ex. A ¶ 10. Moreover, two plaintiffs—Erin Tallman and Michael McCarthy—were not even impacted at all by the breach. *Id.* ¶ 10.

Fourth, at least seven Plaintiffs have had PII disclosed in other data breaches. Ex. A ¶ 12; Ex. B ¶ 34. Indeed, Plaintiff Smith's PII has been involved in at least *thirteen* other data breaches involving companies other than Flagstar. These Plaintiffs therefore cannot tie their purported injuries to the Cyber Incident.

C. Plaintiffs' Other Purported Injuries Are Neither Cognizable Nor Traceable to the Cyber Incident.

1. Alleged Risk of Future Harm Does Not, Standing Alone, Establish Standing in an Action for Damages.

The Supreme Court recently narrowed Article III standing requirements in *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021) holding that "the mere risk of future harm, standing alone, cannot qualify as a concrete harm" in a suit for damages. *Id.* at 2210-11. There, plaintiffs alleged that TransUnion violated the Fair Credit Reporting Act by adding inaccurate alerts to their credit files, thereby "expos[ing] them to a material risk that the information would be disseminated in the future." *Id.* at 2200, 2210. The Supreme Court rejected this argument, concluding that only once "the risk of future harm materialize[d] and the individual suffer[ed] a concrete harm" could plaintiffs have standing to pursue a claim for damages. *Id.* at 2211; *see also Ward v. Nat'l Patient Acct. Servs. Sols., Inc.*, 9 F.4th 357, 361 (6th Cir. 2021) ("[P]laintiffs must demonstrate that . . . 'the risk of future harm materialized,' or that the plaintiffs 'were independently harmed by their exposure to the risk itself.'" (quoting *TransUnion*, 141 S. Ct. at 2211)).

Here, Plaintiffs' allegation—that they face a "certain, imminent, and ongoing threat of fraud and identity theft"—runs headlong into *TransUnion*. Compl. ¶ 86, PageID.586. That risk—even if it existed—cannot create standing on its own. Plaintiffs cannot plausibly allege that the risk of identity theft has

materialized, so they lack standing to pursue claims for damages based on risk of future harm alone. *See Quintero v. Metro Santurce, Inc.*, No. 20-01075-WGY, 2021 WL 5855752, at *5, 8 (D.P.R. Dec. 9, 2021) (concluding that in a ransomware attack, "[a]bsent plausible allegations that the information itself was accessed and misused," plaintiffs lack standing because "the injury is not actual or imminent, but rather is merely conjectural or hypothetical").

2. An Increased Risk of Harm That Is Not Certainly Impending Does Not Establish Standing for Injunctive Relief.

"Allegations of *possible* future injury do not satisfy the requirements of Art. III." *Whitmore v. Arkansas*, 495 U.S. 149, 155 (1990) (emphasis added). Indeed, even an "objectively reasonable likelihood" that an injury will materialize does not suffice. *Clapper*, 568 U.S. at 410. A future injury only establishes standing if "the risk of harm is sufficiently imminent and substantial." *TransUnion*, 141 S. Ct. at 2210. A plaintiff may not rely on speculation to establish this risk. *Id.* at 2211-12.

The future harm that Plaintiffs allege is not "certainly impending" as it "relies on a highly attenuated chain of possibilities" that are belied by the facts of this case. *Clapper*, 568 U.S. at 410, 414.

> Plaintiffs will suffer harm only *if* the hackers actually intend to use Plaintiffs' PII to commit identity theft, fraud, or some other act that might harm Plaintiffs; *if* the hackers attempt to use the PII to commit such identity theft, fraud, or other act; *if* they actually succeed in doing so; and *if* the identity theft, fraud, or other act causes harm to Plaintiffs.

Duqum v. Scottrade, Inc., No. 4:15-CV-1537-SPM, 2016 WL 3683001, at *4 (E.D. Mo. July 12, 2016). Here, there are no plausible allegations that the cyber criminals used Plaintiffs' PII to commit identity theft or fraud. And extrinsic evidence confirms that the Cyber Incident involved a ransomware attack, the primary purpose of which, courts have recognized, "is the exchange of money for access to data, not identity theft." *In re Practicefirst Data Breach Litig*., No. 1:21-CV-00790(JLS/MJR), 2022 WL 354544, at *5 (W.D.N.Y. Feb. 2, 2022), report and recommendation adopted, No. 21-CV-790(JLS), 2022 WL 3045319 (W.D.N.Y. Aug. 1, 2022); *see also Graham v. Universal Health Serv., Inc*., 539 F. Supp. 3d 481, 487 (E.D. Pa. 2021) (observing that the misappropriation of data in a ransomware attack "is generally the means to an end: extorting payment"). Flagstar paid the ransom and destroyed the data, so there is no imminent risk of identity theft or fraud. *See In re Practicefirst Data Breach Litig*., 2022 WL 354544, at *5 (no imminent risk of harm in ransomware incident where hackers copied the data and then deleted it because it was not "the type of cyber-attack targeted to obtain confidential information for purposes of identity theft"); *Graham*, 539 F. Supp. 3d at 487 (no imminent risk of harm resulting from ransomware attack because "Plaintiffs' risk of identity theft 'is dependent on entirely speculative, future actions of an unknown third-party'" (quoting *Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3d Cir. 2011))).

Plaintiffs also fail to allege a basis for injunctive or declaratory relief. Although "a person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring," *TransUnion*, 141 S. Ct. at 2210, future changes to Flagstar's data security will have no impact on any harm that Plaintiffs could potentially suffer as a result of the past Cyber Incident. And "[a]bsent a sufficient likelihood that [Plaintiffs] will again be wronged in a similar way," *City of Los Angeles v. Lyons*, 461 U.S. 95, 111 (1983), past events, like the Cyber Incident, "are not sufficient to confer standing to seek injunctive relief." *Beck v. McDonald*, 848 F.3d 262, 277 (4th Cir. 2017); *Lochridge v. Quality Temp. Servs., Inc.*, No. 22-CV-12086, 2023 WL 4303577, at *8 (E.D. Mich. June 30, 2023) (no standing for declaratory or injunctive relief where plaintiff did not allege facts showing "that a second data breach is currently impending or there is a substantial risk that one will occur").

3. Plaintiffs' Other Alleged Injuries Are Also Insufficient to Confer Article III Standing.

(a) Time and Money Spent Monitoring

Without a plausible risk of future identity theft, Plaintiffs resort to claiming they lost time monitoring their accounts and credit reports, and Plaintiffs Worton and Turner allege that they purchased identity theft and credit monitoring services as a result of the Cyber Incident. Compl. ¶¶ 14, 18, PageID.552, 554-55. Plaintiffs, however, "cannot manufacture standing merely by inflicting harm on themselves

based on their fears of hypothetical future harm that is not certainly impending." *Clapper*, 568 U.S. at 416; *see also Garland v. Orlans, PC*, 999 F.3d 432, 441 (6th Cir. 2021) ("Self-inflicted injuries fail . . . because they are, 'by definition, . . . not traceable to anyone but the plaintiff.'" (citation omitted)).

While the Sixth Circuit held in an unpublished, pre-*TransUnion* decision that a "substantial risk of harm, coupled with reasonably incurred mitigation costs" is enough to establish a cognizable injury, that decision was based on the assumption that a "certainly impending" risk of future harm alone sufficed to establish standing in a suit for damages. *Galaria v. Nationwide Mut. Ins.*, 663 F. App'x 384, 388, (6th Cir. 2016). The Supreme Court has now clarified that a risk of future harm—even if certainly impending—is *not* sufficient to confer standing in a suit for damages. *TransUnion*, 141 S. Ct. at 2211. Plaintiffs' mitigation efforts are, therefore, not enough to establish injury.

Even if *Galaria* remains good law following *TransUnion*, Plaintiffs have not established that they face a "substantial risk" of future harm. Indeed, the fact that the Cyber Incident involved a "garden-variety ransomware attack" as opposed to a "cyber-attack targeted to obtain confidential information for purposes of identity theft," *In re Practicefirst Data Breach Litig.*, 2022 WL 354544, at *5, distinguishes this case from *Galaria* where the court reasoned that "[w]here a data breach targets personal information, a reasonable inference can be drawn that the

hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaints." *Galaria*, 663 F. App'x at 388.

Because the Cyber Incident involved a ransomware attack—where the primary purpose is extortion, not identity theft—the inference that data theft triggers a substantial risk of future harm does not hold. That is even more true here because Flagstar paid the ransom, so the cyber criminals do not even possess the data at issue. *Cf. Shepherd v. Cancer & Hematology Centers of W. Michigan, P.C.*, No. 1:22-CV-734, 2023 WL 4056342, at *6 (W.D. Mich. Feb. 28, 2023) (distinguishing *Galaria* from case where plaintiff's data was not compromised in data breach); *see also Legg*, 574 F. Supp. 3d at 994 ("[W]hile it may have been reasonable to take some steps to mitigate the risks associated with the data breach, those actions cannot create a concrete injury where there is no imminent threat of harm."); *In re SuperValu, Inc., Customer Data Sec. Breach Litig.*, 870 F.3d 763, 771 (8th Cir. 2017) ("Because plaintiffs have not alleged a substantial risk of future identity theft, the time they spent protecting themselves against this speculative threat cannot create an injury.").

Plaintiffs, moreover, cannot establish that mitigation costs were reasonably incurred because Flagstar offered Plaintiffs two years of free credit monitoring services, fraud consultation services, and identity theft restoration. *Dearing v. Magellan Health Inc.*, No. CV-20-00747-PHX-SPL, 2020 WL 7041059, at *3

(D. Ariz. Sept. 3, 2020) ("Defendant offered Plaintiff free personal information protection immediately after the breach . . . . Plaintiff's unnecessary expenditures are not an injury giving rise to standing.").

(b) Diminution in Value of PII

PII has no cognizable monetary value for its owners, and Plaintiffs offer no allegation to the contrary. *See* Compl. ¶¶ 23, 79, PageID.557-58, 582. Courts uniformly hold that diminution in value of PII is not an injury in fact. *See, e.g.*, *Stamat v. Grandizio Wilkins Little & Matthews, LLP*, No. CV SAG-22-00747, 2022 WL 3919685, at *7 (D. Md. Aug. 31, 2022) ("[T]hat someone else can profit from having access to his [PII] does not necessarily lower the value of that [PII] to [plaintiff]."); *Fero v. Excellus Health Plan, Inc.*, 236 F. Supp. 3d 735, 755 (W.D.N.Y. 2017).

Even if PII carries independent monetary value (which it does not), Plaintiffs fail to allege that the diminution harmed them specifically. Nowhere do Plaintiffs allege that they intended to sell their PII but could not, or that they were forced to accept a discounted price. *See, e.g.*, *Welborn v. IRS*, 218 F. Supp. 3d 64, 78 (D.D.C. 2016) (no standing where plaintiffs failed to allege facts showing "that their personal information became less valuable as a result of the IRS breach"). And since Plaintiffs' data has not been disseminated in this ransomware attack, they could not convincingly do so. *See* Ex. A ¶ 6.

(c) Loss of Privacy

"Courts have held that loss of privacy" following a data incident is "too abstract to establish Article III standing." *Duqum*, 2016 WL 3683001, at *8; *see also Darnell v. Wyndham Cap. Mortg., Inc.*, No. 3:20-CV-00690-FDW-DSC, 2021 WL 1124792, at *5 (W.D.N.C. Mar. 24, 2021). That principle holds especially here with a ransomware attack that did not lead to data leaks. *See Patterson v. Med. Rev. Inst. of Am., LLC*, No. 22-CV-00413-MMC, 2022 WL 2267673, at *3 (N.D. Cal. June 23, 2022) (no privacy injury where ransom was paid and the hackers returned the data); *In re Practicefirst Data Breach Litig.*, 2022 WL 354544, at *8 (no privacy injury where there was no allegation that the data held for ransom was ever viewed by an unauthorized person or publicly disclosed).

(d) Overpayment, Loss of Benefit of the Bargain, and Flagstar's "Retention of Profits" Attributable to PII

Courts routinely "reject[] an 'overpayment' theory of damages as an injury-in-fact for standing purposes." *In re: Cmty. Health Sys., Inc.*, 2016 WL 4732630, at *8; *see also, e.g., In re SAIC Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 30 (D.D.C. 2014) ("To the extent that Plaintiffs claim that some indeterminate part of their premiums went toward paying for security measures, such a claim is too flimsy to support standing."). To the extent Plaintiffs paid any money to Flagstar in exchange for banking or mortgage services—though none is actually alleged in the Complaint—Plaintiffs have not alleged that the market value of the services they

received was less than what they paid. Accordingly, this alleged injury cannot serve as a basis for standing.

* * *

In sum, all Plaintiffs fail to adequately plead a cognizable injury that is traceable to the Cyber Incident, and extrinsic evidence confirms that no such injury exists. The Complaint should therefore be dismissed for lack of standing.

II. The Complaint Should Be Dismissed Under Rule 12(b)(6) for Failure to State a Claim.

The Complaint should be dismissed under Rule 12(b)(6) because none of Plaintiffs' causes of action states a plausible claim for relief under applicable law.

A. Choice of Law

Plaintiffs—who are residents of seven states, including Michigan—purport to bring certain common law claims on behalf of a nationwide class. A federal court sitting in diversity applies the choice-of-law rules of the forum state. *See Montgomery v. Wyeth*, 580 F.3d 455, 459 (6th Cir. 2009). For each of the common law claims, Michigan's choice-of-law rules offer two possible options: (1) Michigan law, or (2) the law of each Plaintiff's home state.

For tort claims, Michigan law applies unless there is a "rational reason" to apply the law of another state. *Sutherland v. Kennington Truck Serv.*, 454 Mich. 274, 286 (Mich. 1997). In general, "Michigan has a strong interest in regulating the conduct of companies, especially banks, that hold a public trust, and which

are chartered under its laws." *Allstate Imaging, Inc. v. First Indep. Bank*, No. 2:08-CV-11363, 2010 WL 1524058, at *2 (E.D. Mich. Apr. 15, 2010). For contract claims, Michigan applies the Restatement (Second) of Conflict of Laws, under which the law of the state with the "most significant relationship to the transaction and the parties" applies (absent a choice of law provision). *Chrysler Corp. v. Skyline Indus. Servs., Inc.*, 448 Mich. 113, 121, 528 N.W.2d 698, 701 (Mich. 1995). The factors to be considered are the places of (a) contracting, (b) negotiation, (c) performance, (d) the location of the subject matter of the contract, and (e) the location of the parties. *Id.* at 128 n.35.

This Brief analyzes Michigan law, and to the extent there are any material differences between that and the laws of Plaintiffs' home states, they are noted.

B. Plaintiffs' Negligence Claims Fail.

To state a claim for negligence Plaintiffs must allege: (1) a duty of care, (2) breach of that duty, (3) injury, and (4) causation. *See Doe v. Henry Ford Health Sys.*, 308 Mich. App. 592, 600, 865 N.W.2d 915, 921 (2014). Here, Plaintiffs' negligence claims fail for four reasons: (1) Plaintiffs fail to adequately allege any negligent act or omission by Flagstar, (2) negligence per se is not an independent cause of action, (3) most Plaintiffs fail to allege cognizable injuries, and (4) all Plaintiffs fail to plausibly allege a causal link between any purported negligent act by Flagstar and their alleged injuries.

1. Plaintiffs Have Not Adequately Alleged Any Negligent Act or Omission by Flagstar.

Plaintiffs' negligence claim fails because the Complaint contains nothing more than conclusory allegations that Flagstar breached its duty of care by failing to implement adequate security measures. *See, e.g.*, Compl. ¶ 113, PageID.597-98 (alleging that Flagstar failed to "exercise reasonable care and implement adequate security systems, protocols and practices"). The Complaint contains "no facts regarding any specific measures that [Flagstar] did or didn't take, nor does it contain any allegations regarding the manner in which [Flagstar's] systems were breached." *In re Waste Mgmt. Data Breach Litig.*, Nos. 21CV6147 (DLC), 21CV6199 (DLC), 21CV6257 (DLC), 21CV6902 (DLC), 2022 WL 561734, at *5 (S.D.N.Y. Feb. 24, 2022), *appeal filed*, No. 22-641 (2d Cir. Mar. 25, 2022). Plaintiffs' inability to plausibly allege any facts supporting their conclusory allegations is fatal to the negligence claim. *See id.* (dismissing negligence claim because "[a] conclusory allegation that the defendant acted unreasonably is insufficient to state a claim for negligence").

2. Negligence Per Se Is Not an Independent Cause of Action.

"The weight of Michigan authority supports [the] position that negligence per se is not an independent cause of action, but rather a burden-shifting mechanism within the theory of negligence." *Abnet v. Coca-Cola Co.*, 786 F. Supp. 2d 1341, 1345 (W.D. Mich. 2011). "Plaintiffs may offer evidence of

statutory violations to establish a prima facie case under their claim of negligence . . . but Plaintiffs may not maintain a separate claim of negligence per se." *Id.*; *see also Hardin v. Bank of Am., N.A.*, No. 2:22-CV-10023, 2022 WL 3568568, at *6 (E.D. Mich. Aug. 18, 2022).[6]

Even if negligence per se is an independent cause of action, the Court should still dismiss because (1) alleged violations of statutes that do not provide a private right of action—like Section 5 of the Federal Trade Commission ("FTC") Act and the Gramm-Leach-Bliley Act ("GLBA")—cannot support a claim for negligence per se,[7] and (2) Plaintiffs allege nothing more than conclusory allegations that Flagstar violated Section 5 of the FTC Act, the GLBA, the GLBA's Privacy Rule and/or Regulation P, or the GLBA's Safeguards Rule. *See, e.g.*, Compl. ¶ 121, 124, PageID.600, 601.

3. The Majority of Plaintiffs Fail to Allege Cognizable Injuries.

"[I]t is well settled that, in Michigan, the injury complained of in a

---

[6] Negligence per se is an independent cause of action under Colorado, Missouri, Florida, and Indiana law. *See Gordon v. Chipotle Mexican Grill, Inc.*, 17-CV-1415-CMA-MLC, 2018 WL 3653173, at *19 (D. Colo. Aug. 1, 2018), report and recommendation adopted in part, rejected in part, 344 F. Supp. 3d 1231 (D. Colo. 2018); *In re Brinker Data Incident Litig.*, No. 3:18-CV-686-J-32MCR, 2020 WL 691848, at *9 (M.D. Fla. Jan. 27, 2020); *Am. United Life Ins. Co. v. Douglas*, 808 N.E.2d 690, 704 (Ind. Ct. App. 2004).

[7] *See, e.g.*, *In re Brinker Data Incident Litig.*, 2020 WL 691848, at *9 ("[V]iolation of the FTC Act cannot be the basis for a negligence per se claim.").

negligence action must be an actual, present injury." *Doe*, 308 Mich. App. at 600, 865 N.W.2d at 921 (citation omitted). The negligence claims of Plaintiffs Kennedy, Tallman, Wiedder, McCarthy, Hernandez, Worton, Turner, and McLaughlin must be dismissed because these Plaintiffs have not alleged any actual, present injuries.

Risk of Future Harm. "It is a *present* injury, not fear of an injury in the future, that gives rise to a cause of action under negligence theory." *Doe*, 308 Mich. App. at 600, 865 N.W.2d at 921 (citation omitted). Allegations that a defendant's negligence caused an imminent risk of future harm thus fall short for a negligence claim. *Rakyta v. Munson Healthcare*, No. 354831, 2021 WL 4808339, at *7 (Mich. Ct. App. Oct. 14, 2021) (unpublished opinion).

Lost Time and Resources. Relatedly, damages incurred in anticipation of a possible future injury, rather than in response to present injuries, are not cognizable under Michigan law. *Doe*, 308 Mich. App. At 600, 865 N.W.2d at 921; *Rakyta*, 2021 WL 4808339, at *6-7 (dismissing tort claims and breach of express and implied contract claims based on allegations of lost time and resources to mitigate a potential future injury).

Diminution in value of PII and Privacy. Plaintiffs' allegations that their confidential information lost value as a result of exposure to third parties is conclusory. *Rakyta*, 2021 WL 4808339, at *5; *see also Griffey v. Magellan Health*

Inc., 562 F. Supp. 3d 34, 45 (D. Ariz. 2021) ("[G]eneral allegations that a plaintiff's personal information has diminished in value are not enough" to survive a motion to dismiss). Indeed, the unauthorized viewing of confidential information does not by itself reduce the value of PII, it is the use of the information in some harmful way that devalues the information or otherwise causes harm. *Rakyta*, 2021 WL 4808339, at *5; *see also Provost v. Aptos, Inc.*, No. 1:17-CV-02120-ELR, 2018 WL 1465766, at *4, 6 (N.D. Ga. Mar. 12, 2018) (dismissing claims where plaintiff failed to allege any facts explaining how her PII is less valuable than it was before the breach).

Overpayment/Loss of Benefit of the Bargain. Overpayment and lost benefit of the bargain are not cognizable damages for a negligence claim. *See Attias v. CareFirst, Inc.*, 365 F. Supp. 3d 1, 13 (D.D.C. Jan. 30, 2019) (plaintiffs failed to state a claim for actual damages under a benefit-of-the-bargain theory where plaintiffs broadly alleged that some indeterminate amount of their health insurance premiums went towards providing data security); *see also In re: Cmty. Health Sys., Inc.*, 2016 WL 4732630, at *8 ("[A] number of courts have rejected an 'overpayment' theory of damages as an injury-in-fact for standing purposes.").

Unwanted Communications. Allegations by certain Plaintiffs that they experienced an increase in suspicious spam calls, texts, mail, and/or solicitations following the breach, Compl. ¶¶ 10-12, 18, PageID.549-51, 554-55, are

insufficient to sustain a negligence claim. *See Cooper*, 2022 WL 170622, at *5 ("Courts have generally rejected the theory that unsolicited calls or emails constitute an injury in fact.") (collecting cases); *see also supra* Section I.A.

* * *

Because Plaintiffs Kennedy, Tallman, Wiedder, McCarthy, Hernandez, Worton, Turner, and McLaughlin fail to allege any cognizable injuries, their negligence claims should be dismissed.

4. Plaintiffs Have Not Alleged a Sufficient Causal Link Between Any Negligent Act by Flagstar and Their Alleged Injuries.

All Plaintiffs fail to adequately allege that their purported injuries were *caused by* Flagstar. Under Michigan law, causation requires both cause in fact—that the harmful result would not have come about but for the defendant's negligent conduct—and proximate cause—which examines the foreseeability of consequences. *Haliw v. Sterling Heights*, 464 Mich. 297, 310 (2001).

As discussed in Section I.A, Plaintiffs fail to allege any facts connecting their alleged "injuries" to the Cyber Incident—Plaintiffs do not allege the specific PII that was allegedly compromised in the Cyber Incident, when the purported misuse of their PII occurred, or that their PII has not been previously compromised in other security incidents. Instead, Plaintiffs rely on the phrase "as a result of the data breach" to establish causation which, without additional facts, is too remote and too

speculative to show causation.[8]

C. Plaintiffs' Breach of Confidence Claim Fails.

Plaintiffs' breach of confidence claim should be dismissed because Michigan, like many states, does not recognize such a claim outside of the trade secret context. *Accord Schwartz v. Gilbert*, No. 279992, 2009 WL 416792 (Mich. Ct. App. Feb. 19, 2009) (unpublished opinion) (concluding that breach of confidence claim against a health care provider is properly characterized as one for medical malpractice).

And even if Michigan did recognize such a claim, it would still fail because Flagstar did not intentionally or voluntarily disclose Plaintiffs' PII. *See In re Brinker Data Incident Litig.*, 2020 WL 691848, at *21–22 (dismissing breach of confidence claim under Florida law because plaintiff's information was not disclosed by defendant but rather stolen by third parties).[9]

---

[8] Plaintiffs' other tort claims—breach of confidence and invasion of privacy—should also be dismissed for failure to plead cognizable damages caused by Flagstar. *See Rakyta*, 2021 WL 4808339, at *6 ("[t]o establish a tort claim under Michigan law, the plaintiff must demonstrate a present injury" and affirming dismissal of invasion of privacy claim for failure to plead cognizable damages).

[9] *See also Mackey v. Belden, Inc.*, No. 4:21-CV-00149-JAR, 2021 WL 3363174, at *9 (E.D. Mo. Aug. 3, 2021) (dismissing breach of confidence claim in data breach action because under Missouri law, such claims "are clearly limited to disclosure or communication of trade secrets or other confidential business information"). California and Florida recognize breach of confidence as a separate cause of action, but require that the disclosure be intentional to state a claim. *See In re Ambry Genetics Data Breach Litig.*, 567 F. Supp. 3d 1130, 1146 (C.D. Cal.

(cont'd)

D. Plaintiffs' Invasion of Privacy Claim Fails.

Invasion of privacy is an intentional tort, and thus does not apply where, as here, the defendant is accused of negligence. While Plaintiffs purport to bring an invasion of privacy claim based on intrusion upon seclusion, "the alleged wrongful actions that form the basis of [P]laintiffs' claim of intrusion relate only to the publication [or disclosure] of information, not to any wrongful intrusion." *Doe v. Mills*, 212 Mich. App. 73, 88, 536 N.W.2d 824, 832 (1995) ("An action for intrusion upon seclusion focuses on the manner in which information is obtained, not its publication; it is considered analogous to a trespass."); *see also* Compl. ¶ 160, PageID.610 ("Flagstar intentionally intruded into Plaintiffs' and Class Members' seclusion *by disclosing* without permission their PII to a third party." (emphasis added)).

Michigan law is clear that "to establish an invasion of privacy through the disclosure of private facts, a plaintiff must show that the disclosure of those facts was intentional" and that the information was communicated "to the public at large." *Doe*, 308 Mich. App. at 598, 865 N.S.2d at 920.[10] Here, Plaintiffs have not alleged—and cannot allege—that Flagstar intentionally disclosed their PII to a

---

2021); *In re Brinker Data Incident Litig.*, 2020 WL 691848, at *21–22.

[10] *See also, e.g.*, *Ruiz v. Gap, Inc.*, 380 F. App'x 689, 692–93 (9th Cir. 2010); *Purrelli v. State Farm Fire & Cas. Co.*, 698 So. 2d 618, 620 (Fla. Dist. Ct. App. 1997); *Damner v. Facebook Inc.*, No. 20-CV-05177-JCS, 2020 WL 7862706, at *6 (N.D. Cal. Dec. 31, 2020); *Mackey*, 2021 WL 3363174, at *10.

third party or that their PII has been disseminated to the public. On the contrary, Plaintiffs allege that Flagstar "suffered" a data breach when "cyber criminals infiltrated Flagstar's corporate network" and the data may be on the dark web. Compl. ¶¶ 6, 32-33, PageID.547, 562.

E. Plaintiffs' Breach of Contract Claims Fail.

To state a breach of contract claim, a plaintiff must plead (1) the existence of a valid contract, (2) breach, and (3) damages. *See Doe*, 308 Mich. App. at 601, 865 N.W.2d at 921. A valid contract requires "(1) parties competent to contract, (2) a proper subject matter, (3) legal consideration, (4) mutuality of agreement, and (5) mutuality of obligation." *Bank of Am., N.A. v. First Am. Title Ins. Co.*, 499 Mich. 74, 101, 878 N.W.2d 816, 830 (2016) (citation omitted). An implied contract must also satisfy the elements of mutual assent and consideration. *Lowery v. Dep't of Corr.*, 146 Mich. App. 342, 359, 380 N.W.2d 99, 108 (1985). To determine whether mutual assent has occurred, "an objective test is used to examine 'the express words of the parties and their visible acts.'" *Decker v. City of Wyandotte*, No. 236372, 2002 WL 31956958, at *6 (Mich. Ct. App. Dec. 20, 2002) (citation omitted). "Michigan courts will not lightly presume the existence of an enforceable contract because, 'regardless of the equities in a case, the courts cannot make a contract for the parties when none exists.'" *Huntington Nat. Bank v. Daniel J. Aronoff Living Tr.*, 305 Mich. App. 496, 508, 856 N.W.2d 481, 488 (2014)

(citation omitted). Plaintiffs fail to adequately plead any one of the elements of a breach of contract claim.

First, Plaintiffs fail to adequately allege the existence of an express or implied contract. As for their express contract claim, Plaintiffs do not even identify a contract, leaving Flagstar "to guess as to which 'agreement' was actually breached." *Park v. Morgan Stanley & Co.*, No. 2:11-CV-9466-ODW (MRWx), 2012 WL 589653, at *2 (C.D. Cal. Feb. 22, 2012). Indeed, Plaintiffs allege that a contract was formed when they "obtained products or services from Flagstar, or otherwise provided PII to Flagstar" but then cite to privacy policies in effect at the time of, or well after, the Cyber Incident. *See* Compl. ¶ 167, PageID.612 (citing to Flagstar's California Privacy Notice & Policy dated January 1, 2023); *id.* ¶ 168-69, PageID.612-13 (quoting privacy notice "at the time" of the Cyber Incident).

Even if Flagstar could ascertain which privacy policy it purportedly breached, "broad statements of company policy do not generally give rise to contract claims." *Dyer v. Nw. Airlines Corps.*, 334 F. Supp. 2d 1196, 1200 (D.N.D. 2004). Indeed, Plaintiffs fail to allege any legal consideration for the privacy policy.[11] Nor do Plaintiffs allege that they read or relied on the privacy policy.

[11] A mere "promise to perform an existing legal duty"—like "us[ing] security measures that comply with federal law," Compl. ¶ 168, PageID.612—is insufficient consideration. *Emergency Dep't Physicians P.C. v. United Healthcare, Inc.*, 507 F. Supp. 3d 814, 828 (E.D. Mich. 2020); *see also Griffey*, 562 F. Supp. 3d *(cont'd)*

Dyer, 334 F. Supp. 2d at 1200; *Willingham v. Global Payments, Inc.*, No. 1:12-CV-01157-RWS, 2013 WL 440702, *20 (N.D. Ga. Feb. 5, 2013) (dismissing contract claim where plaintiffs did not plead that they "were aware of, much less relied upon, [d]efendant's statements" in its privacy policy "prior to submitting their data" to defendant).

Plaintiffs' implied contract claim fares no better. Plaintiffs do not allege a "meeting of the minds" on any material facts and instead rely on the conclusory allegation that "Flagstar agreed to safeguard and protect the PII of Plaintiffs and Class Members." Compl. ¶ 177, PageID.615. Plaintiffs do not, however, point to any objective facts establishing that Flagstar agreed, without limitation, to safeguard Plaintiffs' PII. Nor do Plaintiffs point to any objective facts showing that Flagstar agreed to "timely and accurately notify" Plaintiffs "if their PII was breached or compromised." *Id.* Courts have found similar allegations to be insufficient to state a claim for breach of contract. *See In re SuperValu Inc.*, 870 F.3d at 771 n.6 (concluding that plaintiffs did not become parties to an implied contract to protect PII simply by giving defendant their payment information); *Cmty. Bank of Trenton v. Schnuck Mkts., Inc.*, No. 15-CV-1125-MJR, 2017 WL 1551330, at *5 (S.D. Ill. May 1, 2017) (dismissing plaintiffs' breach of implied

---

at 52-53 (dismissing implied breach of contract claim premised on privacy policy for lack of consideration).

contract claim because allegations of an "implicit promise" are insufficient to establish an implied relationship), *aff'd* 887 F.3d 803 (7th Cir. 2018).

Second, even if Plaintiffs alleged the existence of a contract—which they have not—the contract would be unenforceable. Under Michigan law, contracts that cannot be completed within one year of formation must be "in writing and signed with an authorized signature by the party" to the contract. MCL 566.132(1)(a); *see also Ralph Roberts Realty LLC v. Tyson*, 2019 WL 6248354, at *3 (Mich. App. Nov. 21, 2019). According to Plaintiffs, the purported contract was formed when Plaintiffs provided their PII to Flagstar, and under federal law, Flagstar is required to maintain customer identifying information for at least five years. *See* 12 CFR § 1020.220(a)(3)(ii). Thus, the purported contract to "safeguard[]" Plaintiffs' PII, Compl. ¶ 179, PageID.615-16, could not be completed within one year and must therefore be in writing and signed by Flagstar.

Third, Plaintiffs' conclusory allegation that Flagstar failed to use safe and secure systems to protect Plaintiffs' information does not give rise to a breach of express or implied contract. *See Kuhns v. Scottrade, Inc.*, 868 F.3d 711, 717-18 (8th Cir. 2017) ("The implied premise that because data was hacked [a defendant's] protections must have been inadequate is a 'naked assertion[] devoid of further factual enhancement' that cannot survive a motion to dismiss." (alteration in original) (quoting *Iqbal*, 556 U.S. at 678)); *Griffey*, 562 F. Supp. 3d

at 51-52 (rejecting premise that "[b]ecause there was a data breach, [defendant's] data security must have been inadequate, which is a breach of the implied contracts"). The claim that Flagstar breached its privacy policy by "sharing" Plaintiffs' PII, Compl. ¶ 170, PageID.613, makes little sense given that Flagstar did not share PII, it was stolen by a hacker.

Finally, as discussed above, Plaintiffs fail to show that they have suffered any damages resulting from the alleged breach. *See Ruiz*, 380 F. App'x at 691–92; *Rakyta*, 2021 WL 4808339, at *7.

F. Plaintiffs' Unjust Enrichment Claim Fails.

To prove "unjust enrichment, a plaintiff must establish (1) the receipt of a benefit by the defendant from the plaintiff and (2) an inequity resulting to the plaintiff because of the retention of the benefit by the defendant." *Morris Pumps v. Centerline Piping, Inc.*, 273 Mich. App. 187, 195 (2006) (citing *Barber v. SMH (US), Inc.*, 202 Mich. App. 366, 375 (1993)). Without an express contract, "the law will imply a contract to prevent unjust enrichment only if the defendant has been unjustly or inequitably enriched at the plaintiff's expense." *Id.* Plaintiffs fail to allege these elements.

First, Plaintiffs do not allege that Flagstar received any benefit from Plaintiffs. Flagstar is required by federal law to obtain certain PII (including name, address, date of birth, and SSN) from customers prior to opening an account. *See*

31 CFR § 1020.220(a)(2)(i). That Flagstar may use PII to also market its services is not sufficient to satisfy the first element of an unjust enrichment claim. *See Lochridge*, 2023 WL 4303577, at *7 (dismissing unjust enrichment claim where Plaintiff alleged that Defendant received monetary benefits "[t]hrough the use of Plaintiff's and Class Member's Private Information" (alteration in original)).

Second, Plaintiffs fail to allege that Flagstar's retention of the purported benefit would be unjust. To the extent that Plaintiffs conferred any monetary benefit on Flagstar—which they did not—Plaintiffs received, in exchange, financial services from Flagstar. *See In re Zappos.com*, No. 3:12-CV-00325-RCJ-VPC, 2013 WL 4830497, at *5 ("[I]t appears undisputed that Defendant provided Plaintiffs a benefit in return, providing the goods such that there is no unrecompensed benefit conferred.").

G. Plaintiffs' Declaratory Judgment Claim Fails.

The declaratory judgment claim should be dismissed because the Declaratory Judgment Act "does not create an independent cause of action, but rather acts as a remedy for existing cases or controversies." *Lochridge*, 2023 WL 4303577, at *8 (citation omitted). And even if it was an independent cause of action, the claim would still fail because Plaintiffs have not alleged facts showing that a threatened injury—such as another data breach—is certainly impending and therefore lack standing. *See supra* Section I.C.2.

H. Plaintiffs' Statutory Claims Fail.

1. The California Consumer Privacy Act Claim Fails.

To state a claim under the California Consumer Privacy Act ("CCPA"), California Plaintiffs must plausibly allege facts showing that their personal information was "subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information." Cal. Civ. Code § 1798.150(a)(1). Conclusory allegations that fail to "support the notion that Defendant's security was deficient" are insufficient to support a CCPA claim. *Maag v. U.S. Bank Nat'l Ass'n*, No. 21 CV 00031, 2021 WL 5605278, at *2 (S.D. Cal. April 8, 2021) (dismissing CCPA claim).

California Plaintiffs' allegations are precisely the kind of "[t]hreadbare recitals of the elements of a cause of action" that fall short of stating a claim. *Iqbal*, 556 U.S. at 678 (2009). Plaintiffs merely parrot the language of the CCPA, Compl. ¶ 194, PageID.620, and make conclusory allegations that the breach *suggests* that Flagstar failed to follow best cybersecurity practices. *See, e.g.*, Compl. ¶ 76, PageID.581 ("Flagstar's failure to safeguard its customers' PII *suggests* failure to fully comply with industry-standard cybersecurity practices." (emphasis added)). Plaintiffs' proposition that Flagstar's "data security was inadequate simply because there was a data breach . . . is conclusory" and dismissal of the CCPA claim is

therefore warranted. *Griffey*, 562 F. Supp. 3d at 57.

The claim for statutory damages under the CCPA also fails because California Plaintiffs failed to follow the statute's pre-suit notice requirement, which requires a consumer, "prior to initiating any action against a business for statutory damages on an individual or class-wide basis, [to] provide[] a business 30 days' written notice." Cal. Civ. Code § 1798.150(b). Plaintiff Wiedder mailed a notice letter to Flagstar on June 28, 2022, the same day he filed his complaint, and Plaintiff Smith mailed a notice letter to Flagstar on June 30, 2022, the day *after* he filed his complaint.[12] Plaintiffs Kennedy and Tallman neglected to send Flagstar a notice letter at all. None of the California Plaintiffs thus satisfied the "30-days' written notice [requirement] . . . before initiating litigation." *Griffey v. Magellan Health Inc.*, No. CV-20-01282-PHX-MTL, 2022 WL 1811165, at *6 (D. Ariz. June 2, 2022) (dismissing CCPA claim and observing that "if a notice filed before the 30-day deadline could be updated when an amended complaint is filed and satisfy the 30-day notice requirement, then having the pre-suit notice requirement would be pointless").[13] The Court should therefore dismiss the claim for statutory

---

[12] *See* Compl. ¶ 197, PageID.621; Complaint for Damages and Injunctive Relief, *Wiedder v. Flagstar Bank, FSB*, No. 4:22-CV-11446 (E.D. Mich. June 28, 2022), ECF No. 1. *See* Class Action Complaint, *Smith v. Flagstar Bancorp, Inc. et al.*, No. 4:22-CV-11465, PageID.50-52, ¶¶ 154-62 (E.D. Mich. June 29, 2022), ECF No. 1.

[13] Notably, the California legislature could have included a provision in the *(cont'd)*

damages under the CCPA.

2. Plaintiffs Fail to State a Claim for Violation of State Disclosure Laws.

(a) The Claims Under the California Customer Records Act and Washington Data Breach Disclosure Law Fail.

To state a claim under the California Customer Records Act ("CCRA") and Washington Data Breach Disclosure Law ("WDBDL"), Plaintiffs must allege (1) that they were injured by a delayed notice, not just intrusion itself, and (2) that the delayed notice was "unreasonable." *Grigsby v. Valve Corp.*, No. C12-0553JLR, 2013 WL 12310666, at *5 (W.D. Wash., Mar. 18, 2013); *In re Sony Gaming Networks*, 996 F. Supp. 2d at 1010. Plaintiffs fail on both fronts.[14]

First, the California and Washington Plaintiffs do not allege that any of their injuries happened because of delayed notice. *See* Compl. ¶ 86, PageID.586. For example, the Complaint alleges that "timely, adequate notification was required" so that Plaintiffs could "avoid unauthorized charges to their credit or debit card

---

CCPA allowing for amendment of a complaint after compliance with the 30-day notice period, as it did for the CLRA, but did not. *See* Cal. Civ. Code § 1782(d) (providing that "[n]ot less than 30 days after the commencement of an action for injunctive relief, and after compliance with" the 30-day notice period, "the consumer may amend his or her complaint without leave of court to include a request for damages").

[14] The CCRA claim also fails to the extent it relies on Cal. Civ. Code § 1798.81.5, which does not apply to financial institutions, like Flagstar. *See* Cal. Civ. Code § 1798.81.5(e)(2); Compl. ¶¶ 56, 72, 73, 112, PageID.571-72, 579-80, 597.

accounts." Compl. ¶ 112, PageID.597. But at no point do California and Washington Plaintiffs allege they were subject to any unauthorized charges, let alone unauthorized charges that were the result of delayed notification. So too for the rest of their alleged injuries—Plaintiffs never allege any actual injury that would have been avoided or otherwise mitigated by more timely notice. Because a plaintiff "must allege actual damages flowing from the unreasonable delay (and not just the intrusion itself)," these claims should be dismissed. *In re Sony Gaming Networks*, 996 F. Supp. 2d at 1010 (dismissing CCRA claim for failure to allege injury from delayed notification); *see also Grigsby*, 2013 WL 12310666, at *5 (same for WDBDL claim).

Second, the CCRA and WDBDL claims fail because the Complaint does not allege that any purported delay in disclosure was unreasonable. Both statutes allow for delays for "measures necessary to determine the scope of the breach." Cal. Civ. Code § 1798.82(a); Wash. Rev. Code § 19.255.010(8). As Plaintiffs acknowledge, Flagstar did not finish its forensic investigation of the breach until June 2, 2022, just 15 days before Flagstar disclosed the breach. Compl. ¶ 36, PageID.563. Plaintiffs make no effort to allege why this timeline is unreasonable, and instead just repeatedly claim the disclosures were not "timely." *See, e.g.*, Compl. ¶¶ 207–09, PageID.623. Such allegations are conclusory and dismissal is warranted.

(b) The Colorado Security Breach Notifications Act Claim Fails Because There Is No Private Right of Action.

Plaintiff McCarthy cannot state a claim under the Colorado Security Breach Notifications Act ("SBNA") because the Act does not create a private right of action. *See* Colo. Rev. Stat. § 6-1-716(g)(4) (noting only that "[t]he attorney general may bring an action in law or equity to address violations"); *In re Arthur J. Gallagher Data Breach Litig.*, No. 22-CV-137, 2022 WL 4535092, at *15 (N.D. Ill. Sept. 28, 2022) (concluding that the SBNA does not "suppl[y] a private right of action"); *Engl v. Nat. Grocers by Vitamin Cottage, Inc.*, No. 15-CV-02129-MSK-NYW, 2016 WL 8578096, at *12 n.9 (D. Colo. June 20, 2016) (noting that "[d]efendants' argument that the Data Breach Statute does not provide for a private right of action" is "persuasive").

While two courts have deviated from precedent and declined to conclude that no private right of action exists under the SBNA, noting that the statutory language is "ambiguous,"[15] those courts ignore the fact that under Colorado law, courts "will not infer a private right of action based on a statutory violation unless [there is] *clear legislative intent* to create such a cause of action." *Gerrity Oil & Gas Corp. v. Magness*, 946 P.2d 913, 923 (Colo. 1997) (emphasis added). "There

[15] *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1169 (D. Minn. 2014); *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1341 (N.D. Ga. 2019).

is no clear expression of legislative intent" under the SBNA, and therefore the claim should be dismissed. *In re Arthur J. Gallagher*, 2022 WL 4535092, at *15.

Even if a private right of action exists (which it does not), the SBNA claim fails for the same reasons the CCRA and WDBDL claims fail—Plaintiff McCarthy has not alleged that he was injured by the purportedly delayed notice[16] or that any alleged delay was unreasonable. *See* Colo. Rev. Stat. §§ 6-1-716(2)(a).

3. Plaintiffs Fail to State a Claim for Violation of State Consumer Fraud and Unfair and Deceptive Acts and Practices Laws.

The California, Colorado, Indiana, Michigan, and Washington Plaintiffs allege violations of their state consumer fraud and unfair and deceptive acts and practices laws, including: California Unfair Competition Act ("UCL") (Count 11), California Consumer Legal Remedies Act ("CLRA") (Count 12), Colorado Consumer Protection Act ("Colorado CPA") (Count 14), Indiana Deceptive Consumer Sales Act ("IDCSA") (Count 15), Michigan Consumer Protection Act ("MCPA") (Count 16), and Washington Consumer Protection Act ("WCPA") (Count 18). In general, these claims are based on Flagstar's purported failure to implement and maintain reasonable security measures and comply with common law and statutory duties pertaining to the security and privacy of PII, and purported

[16] Notably, Plaintiff McCarthy does not allege that he was notified by Flagstar that his PII was compromised in the breach, Compl. ¶ 12, PageID.551, indicating that he is not part of the putative class.

misrepresentations and omissions regarding the same. *See, e.g.*, Compl. ¶¶ 215-17, PageID.624-27. These claims fail for a variety of reasons.

(a) Plaintiffs Fail to Allege a Cognizable Injury or Loss Caused by the Cyber Incident.

To state a claim under each of these statutes, Plaintiffs must allege a cognizable injury or loss caused by the allegedly deceptive or unfair conduct. *See In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 804 (N.D. Cal. 2019) (under the UCL, "plaintiffs must show that they 'lost money or property' because of [defendants'] conduct"); *Meyer v. Sprint Spectrum L.P.*, 200 P.3d 295, 299 (Cal. 2009) (under CLRA, consumer must allege "some kind of damage" resulting from unlawful practice); Wash. Rev. Code § 19.86.090 (requiring that a person be "injured in his or her business or property by a violation" of the Washington CPA); *Gordon v. Finch*, No.: 2:21-CV-292-TLS-JEM, 2023 WL 3496427, at *8 (May 17, 2023 N.D. Ind.) (noting that the IDCSA permits plaintiffs to "bring an action for the damages actually suffered as a consumer as a result of the deceptive act"); *Donna v. Countrywide Mortg.*, No. 14-CV-03515-CBS, 2015 WL 9456325, at *3 (D. Colo. Dec. 28, 2015) (under Colorado CPA, a plaintiff must allege "that the plaintiff suffered injury in fact"); Mich. Comp. Laws §§ 445.911(2)-(4) (a person must "suffer[] loss as a result of a

violation" of the MCPA).[17]

As explained in Sections I.C and II.B.3, Plaintiffs Kennedy, Tallman, Wiedder, McCarthy, Worton, and McLaughlin allege nothing more than increased risk of future harm, lost time and resources mitigating that risk, diminution in value of PII, overpayment for Flagstar's services, and unwanted communications (Tallman, Wiedder, and McCarthy). These purported injuries are insufficient to state a claim under the statutes at issue. *See, e.g.*, *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 966 (S.D. Cal. 2012) ("[A]llegations that the heightened risk of identity theft, time and money spent on mitigation of that risk, and property value in one's information, do not suffice as injury under the UCL [or] . . . CLRA."); *Aspen Am. Ins. Co. v. Blackbaud, Inc.*, 624 F. Supp. 3d 982, 997-98 (N.D. Ind. 2022) (risk of identity theft and attendant costs to guard against identity theft are not compensable injuries under Indiana law). Plaintiff Smith's UCL claim also fails because he has not alleged any lost money or property, but rather unauthorized attempted bank transfers. *See Jackson v. Loews Hotels, Inc.*, No. ED CV 18-827-DMG (JCx), 2019 WL 6721637, at *4 (C.D. Cal. July 24, 2019) ("'[T]heft' or 'unauthorized release of personal

[17] While the Michigan Plaintiffs purport to bring a claim on behalf of a Michigan Subclass for "the greater of actual damages or $250," Compl. ¶ 273, PageID.644, the MCPA does not allow for statutory damages in a class action. *See* Mich. Comp. Laws Ann. § 445.911(2)-(4).

information' does not qualify as lost money or property for purposes of . . . the UCL."). Further, all Plaintiffs fail to connect their purported injuries to the Cyber Incident, let alone any purported deceptive act by Flagstar. *See* Sections I.A, II.B.4.

(b) Plaintiffs' Fraud-Based Claims Fail.

Each of the consumer protection claims is based, in whole or in part, on purported misrepresentations and omissions.[18] Plaintiffs must therefore satisfy Rule 9(b)'s heightened pleading standard.[19] The fraud-based claims fail for at least three reasons.

First, Plaintiffs fail to set forth the "who, what, when, where, and how" of the alleged fraud. *See In re Zoom Video Commc'ns Inc. Privacy Litig.*, 525 F. Supp. 3d at 1045 (dismissing plaintiffs' fraud-based UCL and CLRA claims because plaintiffs "merely identif[ied] the statements on Zoom's website and privacy policy that are reasonably likely to mislead"). The Complaint is littered

[18] *See, e.g.*¸ Compl. ¶¶ 217-18, 226-27, 244-46, 259, 267-270, 285-86 PageID.626-27, 629-30, 633-35, 639, 641-43, 646-48.

[19] *See In re Zoom Video Commc'ns Inc. Privacy Litig.*, 525 F. Supp. 3d 1017, 1045 (N.D. Cal. 2021) (applying Rule 9(b) to UCL and CLRA fraud-based claims); *Goodwin v. CitiMortgage, Inc.*, No. 1:12–CV–760, 2013 WL 4499003, at *5 (W.D. Mich. Aug. 19, 2013) ("Rule 9(b) . . . is applicable to . . . allegations of fraud under the MCPA."); *Shea v. Gen. Motors LLC*, 567 F. Supp. 3d 1011, 1024 (N.D. Ind. 2021) ("The heightened pleading standard of Rule 9(b) applies to [IDCSA] claims."); *Nemykina v. Old Navy, LLC*, 461 F. Supp. 3d 1054, 1058-59 (W.D. Wash. 2020) ("Rule 9(b) therefore applies to Plaintiff's [W]CPA claims sounding in fraud."); *Donna*, 2015 WL 9456325, at *4 ("To state the element that Defendants engaged in an unfair or deceptive trade practice, [plaintiffs] must fulfill the heightened Rule 9(b) pleading standard.").

with conclusory allegations that Flagstar "misrepresent[ed] that they would protect the privacy and confidentiality of Plaintiffs' . . . PII" and "misrepresent[ed] that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' . . . PII." Compl. ¶ 245(d)-(e), PageID.635; *see also id.* ¶¶ 217(d)-(e), PageID.626-27, 267(d)-(e), PageID.641, 285(d)-(e), PageID.647. Nowhere, however, do Plaintiffs identify *what* those particular misrepresentations were, *who* made the misrepresentations, or *when*, *where*, and *how* they were made.

Second, Plaintiffs fail to allege reliance on the purported misrepresentations and omissions. *See Shain v. Advanced Techs. Grp., LLC*, No. CV 16-10367, 2017 WL 768929, at *11 (E.D. Mich. Feb. 28, 2017) ("[A] plaintiff alleging a violation [of the MCPA or IDCSA] based on material misrepresentations or omissions must show reliance."); *Crowe v. Tull*, 126 P.3d 196, 209-10 (Colo. 2006) (noting that reliance is a factor under the Colorado CPA); *In re Sony*, 903 F. Supp. 2d at 969 (stating that fraud-based claims under UCL and CLRA require plaintiffs to plead "actual reliance").[20] Indeed, at no point do Plaintiffs allege that they ever read, much less relied on, the claimed misrepresentations.

[20] The WCPA does not require actual reliance on the deceptive act, but rather whether the alleged practice was likely to deceive a reasonable consumer. *See In re: Premera Blue Cross Cust. Data Sec. Breach Litig.*, No. 3:15-md-2633-SI, 2017 WL 539578, at *4 (D. Or. Feb. 9, 2017).

Finally, to the extent the claims are premised on purported omissions of material fact, Plaintiffs fail to allege that Flagstar owed them a duty to disclose those facts. *See, e.g.*, *Hendricks v. DSW Shoe Warehouse, Inc.*, 444 F. Supp. 2d. 775, 783 (W.D. Mich. 2006) (dismissing MCPA claim in part because "there is no . . . authority to support plaintiff's position that [defendant] had a legal duty to disclose to is customers . . . specific information about its computer security systems"); *Daugherty v. Am. Honda Motor Co., Inc.*, 51 Cal. Rptr. 3d 118, 126 (Cal. Ct. Appl. 2006) (holding that for a CLRA claim "to be actionable the omission must be contrary to a representation actually made by the defendant, or an omission of a fact the defendant was obliged to disclose"). The IDCSA, moreover, does not apply to omissions. *Shain*, 2017 WL 768929, at *12.

(c) Plaintiffs' "Unfair" and "Unlawful" Practices-Based Claims Fail.

To the extent Plaintiffs allege unfair or unlawful practices in purported violation of the UCL, MCPA, or WCPA, those claims fail because Plaintiffs plead nothing more than conclusory allegations that "Flagstar failed to implement and maintain reasonable security measures" and violated the FTC Act, GLBA, CCRA, and CCPA.[21] As discussed above, the mere fact that the Cyber Incident occurred does not mean that Flagstar failed to maintain reasonable security measures. See

[21] Claims brought under the Colorado CPA and IDCSA must be based on "deceptive" acts. *See* Colo. Rev. Stat. § 6-1-105; Ind. Code § 24-5-0.5-4.

Sections II.B.1 and II.H.1.

(d) California Plaintiffs' UCL Claim Fails Because Plaintiffs Do Not Lack Adequate Legal Remedies.

"Remedies under the UCL are limited to restitution and injunctive relief, and do not include damages." *Silvercrest Realty, Inc. v. Great Am. E&S Ins. Co.*, No. SACV 11-01197-CJC(AN), 2012 WL 13028094, at *2 (C.D. Cal. Apr. 4, 2012). In order to seek restitution under the UCL, a plaintiff must allege "the requisite inadequacy of legal remedies." *Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 844 (9th Cir. 2020); *see also Gardiner v. Walmart Inc.*, No. 20-CV-04618-JSW, 2021 WL 2520103, at *7 (N.D. Cal. Mar. 5, 2021) (dismissing a UCL claim arising from data breach where plaintiffs fail to allege they have no adequate remedies at law). Plaintiffs do not allege that they have no adequate remedy at law.

(e) Plaintiff Worton's IDCSA Claim Fails for Two Additional Reasons.

Plaintiff Worton's IDCSA claim fails for two additional reasons. *First*, where, as here, a consumer has not given written notice of the alleged deceptive act, an action may only be brought under the IDCSA if the "deceptive act is incurable," Ind. Code § 24-5-0.5-5(a), *i.e.*, the deceptive act is "part of a scheme, artifice, or device with intent to defraud or mislead," *id.* § 24-5-0.5-2(a)(8). Here, even if Plaintiff Worton pled a deceptive act with particularity, which he has not, Plaintiff Worton makes no attempt to allege any facts suggesting that Flagstar

acted with intent to defraud or mislead. *Second*, an IDCSA claim cannot be based on purported failure to "timely and accurately disclose the Data Breach to Plaintiff and the Indiana Subclass," Compl. ¶ 259(e), PageID.639, because such a claim is "actionable only by the attorney general." Ind. Code § 24-4.9-4-1.

CONCLUSION

For the foregoing reasons, Defendants respectfully request that the Court grant their Motion to Dismiss the Consolidated Class Action Complaint.

Dated: July 24, 2023

Respectfully submitted,

/s/ William E. Ridgway
William E. Ridgway
Lindsey Sieling
SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP
155 N. Wacker Dr., Suite 2700
Chicago, IL 60606
Telephone: (312) 407-0700
Facsimile: (312) 407-0411
William.Ridgway@skadden.com
Lindsey.Sieling@skadden.com

Sean P. McNally (P66292)
Jason E. Manning
TROUTMAN PEPPER HAMILTON SANDERS LLP
4000 Town Center, Suite 1800
Southfield, MI 48075
Telephone: (248) 359-7300
Sean.McNally@troutman.com
Jason.Manning@troutman.com

Counsel for Defendants

CERTIFICATE OF SERVICE

I hereby certify that on July 24, 2023, I caused a true and correct copy of the foregoing Defendants' Motion to Dismiss the Consolidated Class Action Complaint and Brief in Support thereof to be filed electronically with the Clerk of the Court using the CM/ECF system, which will automatically send notice of such filing to all counsel of record.

/s/ William E. Ridgway
William E. Ridgway